

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
MARSHALL DIVISION**

IN RE: TAASERA LICENSING LLC,  
PATENT LITIGATION

THIS DOCUMENT RELATES TO  
CASE NO. 2:22-cv-00314-JRG

§  
§  
§  
§  
§  
§  
§

Case No. 2:22-md-03042-JRG

**JURY TRIAL DEMANDED**

---

PALO ALTO NETWORKS, INC.,

Plaintiff,

v.

TAASERA LICENSING LLC AND QUEST  
PATENT RESEARCH CORPORATION,

Defendants.

§  
§  
§  
§  
§  
§  
§  
§  
§  
§  
§

Case No. 2:22-cv-00314-JRG

**JURY TRIAL DEMANDED**

**DEFENDANTS TAASERA LICENSING LLC AND  
QUEST PATENT RESEARCH CORPORATION'S CORRECTED RESPONSE  
IN OPPOSITION TO PLAINTIFF PALO ALTO NETWORKS, INC.'S  
MOTION FOR PARTIAL JUDGMENT ON THE PLEADINGS  
OF PATENT-INELIGIBILITY UNDER 35 U.S.C. § 101 (DKT. 71)**

**TABLE OF CONTENTS**

	<b><u>Page(s)</u></b>
I. INTRODUCTION .....	1
II. LEGAL STANDARDS .....	1
III. ARGUMENT .....	3
A. The '796 Patent is Patent-Eligible Under 35 U.S.C. § 101 .....	3
B. The '356 Patent is Patent-Eligible Under 35 U.S.C. § 101 .....	5
C. The '517 Patent is Patent-Eligible Under 35 U.S.C. § 101 .....	9
D. The '038 and '918 Patents are Patent-Eligible Under 35 U.S.C. § 101.....	12
IV. CONCLUSION.....	15

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>Cases</b>	
<i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 882 F.3d 1121 (Fed. Cir. 2018) .....	3
<i>Alice Corp. Pty. Ltd. v. CLS Bank Int’l</i> , 573 U.S. 208 (2014).....	2
<i>Assoc. for Molecular Pathology v. Myriad Genetics, Inc.</i> , 569 U.S. 576 (2013).....	2
<i>Bancorp Servs., L.L.C. v. Sun Life Assur. Co. of Can.</i> , 687 F.3d 1266 (Fed. Cir. 2012) .....	11
<i>Berkheimer v. HP Inc.</i> , 881 F.3d 1360 (Fed. Cir. 2018), <i>cert. denied</i> , No. 18-415, 2020 WL 129532 (Jan. 13, 2020) .....	3, 5
<i>CardioNet, LLC v. InfoBionic, Inc.</i> , 955 F.3d 1358 (Fed. Cir. 2020) .....	3
<i>Cellspin Soft, Inc. v. Fitbit, Inc.</i> , 927 F.3d 1306 (Fed. Cir. 2019) .....	2, 3
<i>Commc’n Interface Techs., LLC v. Albertson’s LLC</i> , No. 4:20-CV-550-SDJ, 2021 WL 4453580 (E.D. Tex. Sept. 29, 2021).....	7
<i>Content Extraction &amp; Transmission LLC v.</i> <i>Wells Fargo Bank, Nat’l Ass’n</i> , 776 F.3d 1343 (Fed. Cir. 2014) .....	4
<i>Dropbox, Inc. v. Synchronoss Techs., Inc.</i> 815 F. App’x 529,532 (Fed. Cir. 2020) .....	10
<i>eCeipt LLC v. Homegoods, Inc.</i> , No. W-19-CV-00032-ADA, 2019 WL 10302271 (W.D. Tex. May 20, 2019) .....	14
<i>Enfish, LLC v. Microsoft Corp.</i> , 822 F.3d 1327 (Fed. Cir. 2016) .....	3, 14, 15
<i>Finjan, Inc. v. Blue Coat Sys., Inc.</i> , 879 F.3d 1299 (Fed. Cir. 2018) .....	9, 15
<i>Intell. Ventures I LLC v. Erie Indem. Co.</i> , 711 F. App’x 1012 (Fed. Cir. 2017) .....	6

<i>Mayo Collaborative Servs. v. Prometheus Lab’ys, Inc.</i> , 566 U.S. 66 (2012).....	2
<i>Microsoft Corp. v. i4i Ltd. P’ship</i> , 564 U.S. 91 (2011).....	2
<i>Miller v. Dep’t of Just.</i> , 842 F.3d 1252 (Fed. Cir. 2016) .....	2
<i>Ollnova Techs. Ltd. v. Ecobee Techs., ULC</i> , No. 2:22-cv-00072, Dkt. 63, 17-18 (E.D. Tex. Sept. 21, 2022) (Slip Op.) .....	5, 11
<i>Price v. Symsek</i> , 988 F.2d 1187 (Fed. Cir. 1993) .....	2
<i>Santosky v. Kramer</i> , 455 U.S. 745 (1982).....	2
<i>Slyce Acquisition Inc. v. Syte-Visual Conception Ltd.</i> , No. W-19-cv-257, 2020 WL 278481 (W.D. Tex. Jan. 10, 2020).....	2
<i>TecSec, Inc. v. Adobe Inc.</i> , 978 F.3d 1278 .....	3, 15
<b>Statutes</b>	
35 U.S.C. § 101.....	<i>passim</i>
35 U.S.C. § 282.....	2

Declaratory-Judgment Plaintiff Palo Alto Networks, Inc.’s (“PAN” or “Plaintiff”) filed this Motion for Partial Judgment on the Pleadings of Patent-Ineligibility Under 35 U.S.C. §101 on December 22, 2022 (Dkt. 71) (the “Motion”) asserting that five of the nine Asserted Patents should be resolved on the pleadings now: (1) U.S. Patent No. 6,842,796 (Ex. 1, the “’796 patent”); (2) U.S. Patent No. 8,127,356 (Ex. 2, the “’356 patent”); (3) U.S. Patent 8,850,517 (Ex. 3, the “’517 patent”); (4) U.S. Patent 8,955,038 (Ex. 4, the “’038 patent”); and (5) U.S. Patent No. 9,923,918 (Ex. 5, the “’918 patent”) (collectively, the “challenged patents”).<sup>1</sup>

## **I. INTRODUCTION**

The inventions claimed in the five patents are all eligible under 35 U.S.C. § 101 because they are not abstract under step one of the *Alice* framework. Each challenged claim is “directed to” concrete improvements in the field of internet security, including solving specific problems that are unique to that technology area. That the majority of the claims are method claims involving the identification, sorting, and extracting of information does not transform the claims into ineligible subject matter. Under step two of the *Alice* framework, PAN cites to no prior art or other information that the claimed elements, alone or in combination, were well-known, routine, and conventional at the time each of the patent applications was filed. This alone dooms the analysis, as questions of fact remain regarding the knowledge of the person of ordinary skill in the art and the state of the art at that time.

## **II. LEGAL STANDARDS**

Patents are presumed valid. *Microsoft Corp. v. i4i Ltd. P’ship*, 564 U.S. 91, 100 (2011)

---

<sup>1</sup> PAN challenges every claim of each challenged patent. But, Taasera has not served its infringement contentions, and there is not yet a listing of asserted claims. It is unclear how PAN has standing to challenge unasserted claims, which highlights the premature nature of PAN’s Motion.

(citing 35 U.S.C. § 282). This presumption of validity extends to patent-eligible subject matter. *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1319 (Fed. Cir. 2019). Overcoming the presumption of validity in an infringement case generally requires clear and convincing evidence, *Microsoft*, 564 U.S. at 95. The clear and convincing standard “has been described as evidence which produces in the mind of the trier of fact an abiding conviction that the truth of a factual contention is ‘highly probable.’” *Miller v. Dep’t of Just.*, 842 F.3d 1252, 1257-58 (Fed. Cir. 2016) (quoting *Price v. Symsek*, 988 F.2d 1187, 1191 (Fed. Cir. 1993)). As other federal courts have noted in the Section 101 context, “clear and convincing evidence is a high bar and the same heightened standard required to terminate a parent-child relationship.” *Slyce Acquisition Inc. v. Syte-Visual Conception Ltd.*, No. W-19-cv-257, 2020 WL 278481, at \*4 n.2 (W.D. Tex. Jan. 10, 2020) (citing *Santosky v. Kramer*, 455 U.S. 745, 769–70 (1982)).

Pursuant to Supreme Court precedent construing 35 U.S.C. § 101, “[l]aws of nature, natural phenomena, and abstract ideas” are ineligible subject matters for patent protection. *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 573 U.S. 208, 216 (2014) (quoting *Assoc. for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 589-90 (2013)). Under the Supreme Court’s two-part test to determine patent eligibility, a court must (1) “determine whether the claims at issue are directed to one of those patent-ineligible concepts,” and (2) if so, “consider the elements of each claim both individually and ‘as an ordered combination’ to determine whether the additional elements ‘transform the nature of the claim’ into a patent-eligible application.” *Alice*, 573 U.S. at 217 (quoting *Mayo Collaborative Servs. v. Prometheus Lab’ys, Inc.*, 566 U.S. 66, 78-79 (2012)).

Rule 12 standards apply to **both** *Alice* steps one and two. At step one, courts must “draw all reasonable inferences” from the intrinsic record, including the specification, in favor of the nonmoving party in determining the focus of the patent. *CardioNet, LLC v. InfoBionic, Inc.*, 955

F.3d 1358, 1371 (Fed. Cir. 2020) (reversing district court for failing to “draw all reasonable inferences” in favor of patentee at *Alice* step one). At step two, “plausible and specific factual allegations that aspects of the claims are inventive are sufficient” to defeat a Rule 12 motion. *Cellspin*, 927 F.3d at 1317-18 (citing *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1126-27 (Fed. Cir. 2018) and *Berkheimer v. HP Inc.*, 881 F.3d 1360 (Fed. Cir. 2018)).

### III. ARGUMENT

#### A. The '796 Patent is Patent-Eligible Under 35 U.S.C. § 101

Claim 1 of the '796 patent (attached as Exhibit 1) is not directed to an abstract idea, nor is the claim directed to well-known, routine, and conventional steps. PAN understands this, stating that, “On its face, claim 1 is directed to the abstract idea of identifying and extracting information from a set of data by matching a pattern.” Motion at 2. This is indicative of the inappropriate view that pervades Defendant’s Motion. Each patent claim is not meant to be viewed “[o]n its face” and reduced to the simplest description in order to determine patentability. The claims are to be read in light of the specification and examined as an ordered combination. The Federal Circuit has repeatedly warned, mischaracterizing a claim, or disregarding its elements, is improper: this results in “‘a high level of abstraction’ that is ‘untethered from the claim language’ and that ‘overgeneraliz[es] the claim.’” *TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278, 1295 ((Fed. Cir. 2020) (citing *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016)) (rejecting Section 101 arguments that disregarded claim elements and ignored the specification).

While Taasera does not agree with PAN’s assertion that Claim 1 is exemplary of all challenged claims, independent Claim 1 is not abstract. It requires:

- “identifying at least one regularly identifiable expression in the input sequence of data symbols, wherein the at least one regularly identifiable expression represents a pattern that is matchable in accordance with a programming language that supports such a regularly identifiable expression”

- “identifying at least a portion of information associated with the at least one regularly identifiable expression”
- “extracting the portion of information.”

Claim 1 requires identifying an expression which “represents a pattern that is matchable in accordance with a programming language.” PAN admits that this cannot be “performed by a human.” Motion at 3. PAN incorrectly reduces the claim to merely “‘identifying’ and ‘extracting’ information,” ignoring the claimed use of “a programming language.” According to the ’796 patent, “there is a need for data processing techniques which explicitly identify portions of data that are sought to be identified, rather than only implicitly identifying, or tagging, such portions of data.” ’796 patent, 1:46-49. The ’796 patent is directed to analyzing “data streams representing DNA (deoxyribonucleic acid) sequences, RNA (ribonucleic acid) sequences, amino-acid sequences, and audio and video sequences that are preprocessed into a discrete symbolic form,” not just documents and voicemails as discussed by PAN. *Id.*, 1:64-67. The inventive concept relates to using a programming language “stored in one or more of the associated memory devices (e.g., ROM, fixed or removable memory) and, when ready to be utilized, loaded in part or in whole (e.g., into RAM) and executed by a CPU” to analyze complex input data and extract portions of information. *Id.*, 12:47-51. Under *Alice* Step One, the claims are not directed to an abstract idea.

PAN’s assertion that the claims invalidated in *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n* are analogous to the claims of the ’796 patent is unsound. 776 F.3d 1343, 1345 (Fed. Cir. 2014). The claims in *Content Extraction* were directed to scanning documents, recognizing portions of the documents “corresponding to a first data field,” and storing it. *Id.* This is precisely what the ’796 patent identifies in the prior art and improves upon by “identify[ing] portions of data in a document that a user seeks to be identified” using a programming language. ’796 patent, 1:54-55.

PAN also alleges that Claim 1 is abstract because “its steps are recited in purely functional terms.” Motion at 3. But PAN mischaracterizes the claim language. The functional term “identifying” is performed by matching with a programming language. PAN’s argument that it is unclear how information is extracted only highlights that claim construction is necessary, not that the claim is abstract. *Id.* Claim 1 of the ’796 patent is also not directed to routine, well-known, and conventional ideas under *Alice* Step Two, and factual issues remain regarding the state of the art at the time the patent was filed. *Ollnova Techs. Ltd. v. Ecobee Techs., ULC*, No. 2:22-cv-00072, Dkt. 63, 17-18 (E.D. Tex. Sept. 21, 2022) (Slip Op.). While the prior art identified in the intrinsic record was able to “identify all occurrences of certain classes of words in a document,” such as “person-names, city-names, dates, and times,” it lacked the ability to “explicitly identify the portions of text that are important.” ’796 patent, 1:26-45. PAN seeks to analogize the inventive concept of the ’796 patent to reviewing bank checks to “recognize[] relevant data such as the amount, account number, and identity of account holder, and store[] that information in the[] records.” Motion at 3. PAN’s comparison ignores the innovative usage of the programming language described in the ’796 patent to “explicitly identify portions of data in a document *that a user seeks* to be identified, *e.g.*, relevant or important information,” (’796 patent, 1:-53-55 (emphasis added)) which was far from well-known, routine, or conventional at the time of the invention and certainly provides “significantly more” that transforms the abstract idea into a patentable invention. *Berkheimer* 881 F.3d at 1368.

#### **B. The ’356 Patent is Patent-Eligible Under 35 U.S.C. § 101**

Here again, Plaintiff’s argument is divorced from the actual language of the claims. The ’356 patent (attached as Exhibit 2) Claim 1 requires:

- “first program instructions to determine if the packet is a known exploit”

- “second program instructions to determine if the packet is addressed to a broadcast IP address of a network”
- “third program instructions to determine if the packet is network administration traffic”
- “fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet is not a new, exploit candidate”
- “fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate”

PAN’s argument is based on an extreme oversimplification which ignores numerous claim limitations. Claim 1 requires a “computer-readable tangible storage device” loaded with program instructions to perform analysis of packets in a network. The program of Claim 1 analyzes packets in a network to determine if they are a “known exploit,” “addressed to a broadcast IP address,” or “network administration traffic,” and based on the determinations whether the packets are new, exploit candidates. The inventive concept under *Alice* Step One is not merely “sorting data . . . based on simple if/then logic,” but rather a processor executing program instructions that automatically determines if a packet is a new, exploit candidate. This is a specific improvement in the identification of new computer viruses, worms, exploitation code, or other unwanted intrusions.

The claims here are not at all related to those in *Erie*, as PAN argues. *Intell. Ventures I LLC v. Erie Indem. Co.*, 711 F. App’x 1012, 1014 (Fed. Cir. 2017). There, the claims were directed to a method to review files stored on a computer “according to pre-set criteria” to help with combatting “great legal risks” from “the presence of certain files (such as depictions of child pornography or copyrighted music files).” *Id.* Once recognized by the “file identification application,” the files were marked for deletion. *Id.* Rather than use a computer to simply perform an activity a human could do, like review a file for offensive material according to pre-set criteria

and mark it for deletion, the inventions of the '356 patent improves the function of the computer itself by solving problems with computer security. The claims here are directed to steps performed by a computer system that automatically analyzes packet data moving through a network to identify new computer viruses, worms, exploits, etc.—steps which could not be performed by a human.

The claims here, like those in *Commc'n Interface Techs., LLC v. Albertson's LLC*, “are directed to improving the functionality of client-server communication systems,” albeit which makes identification of threats on the network faster and more efficient, instead of making “virtual session reconnection faster and more efficient.” No. 4:20-CV-550-SDJ, 2021 WL 4453580, at \*7, \*9 (E.D. Tex. Sept. 29, 2021). There, the claims “recite[d] sending an ‘application-program identifying packet’ in addition to a ‘signal indicative of an incoming communication request’ to the remote unit. The ‘application-program identifying packet’ sent with the client-server communication signal ‘identif[ies] an application program that needs to resume a virtual session,’ thereby ‘placing the virtual session back into the active state and transferring data between the application and the remote unit.’” *Id.* at \*7. The Court held that “[t]hese claim elements, as illuminated by the specification, recite specific improvements over prior technology and thus remove the asserted claims from the realm of abstract ideas.” *Id.*

PAN’s argument that Claim 1 is also abstract because each step recites “program instructions” that “determine” if conditions are met ignores the specification and highlights that claim construction is needed. Motion at 7. For example, to determine if a packet is “broadcast traffic,” the “program 30 determines the gateway IP address and the netmask of the network on which the honeypot resides. This can be gained by system calls to the honeypot. The gateway IP address is the IP address of a router or other device in the network which received the packet from

the Internet and forwarded the packet to the honeypot 12 (and possibly other devices on intranet 14). The netmask indicates how many IP addresses are available in the network, ex. One through sixty four. From the gateway IP address and netmask, program 30 determines whether the destination IP address in the packet header is the broadcast IP for this network.” ’356 patent, 7:45-55. Each claimed determine step is explained in detail in the specification, and it further demonstrates that the claims cannot be performed by a human.

The claims are also not well-known, routine, and conventional under *Alice* Step Two. While a human analyst was capable of analyzing packets in some way, it was “time consuming,” “prone to error,” and detection of attacks, viruses, etc. was delayed. ’356 Patent, 2:66-3:5. Accordingly, the ’356 patent’s solution was to use a computer program in a new way to perform the analysis of packets. Regarding the determination of a “known exploit,” the ’356 patent states:

[A] known intrusion detection system (“IDS”) 22 is connected to the intranet 14 and to honeypot 12. The IDS 22 has a current list of signatures of known viruses, worms, exploitation programs and other exploits. The IDS performs a key word search of the packets it receives, searching for these known signatures. When the IDS detects such an exploit or a portion thereof in a packet it receives based on the presence of the key words in the packet, the IDS sends the packet in an alert or identifies the packet in an alert to program 30 in the honeypot 12. The identification can be in the form of a TCP sequence number of the current packet or the sequence of packets which includes the current packet. The TCP sequence is a sequence of packets that together form one packet.

*Id.*, 6:36-48.

In order to determine whether a packet is network administration traffic, “program 30 determines the IP protocol and IP address of the current packet by parsing the packet header (step 500). Then, program 30 compares the combination of IP protocol and IP address of the current packet to the combinations on the list 33 (step 501). If there is a match (decision 502, yes branch), then the current packet is deemed harmless network administration traffic, and program 30 proceeds to step 102 as described above.” *Id.*, 8:29-36.

The claims here are closely comparable to those in *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299 (Fed. Cir. 2018), where the court addressed a claimed invention involving a method for scanning an application program for viruses, generating a security profile identifying any potentially suspicious code in the program, and linking the security profile to the application program. *Id.* at 1304–05. The court held that the technique for virus scanning claimed in the case constituted an improvement in computer functionality and therefore included an inventive step, making the claims patent eligible. Similarly, here, the new system for analyzing packets for exploits is an improvement to computer functionality, reliability, and safety, and thus includes an inventive step. Accordingly, the invention of a computer system for detecting unknown computer attacks was not well-known, routine, or conventional at the time of the invention and provides “significantly more” that transforms the abstract idea into a patentable invention. *Id.* at 1303.

### **C. The ’517 Patent is Patent-Eligible Under 35 U.S.C. § 101**

Plaintiff mischaracterizes the claims of the ’517 patent (attached as Exhibit 3) as merely “assigning a score based on risk.” Motion at 1, 10. Plaintiff ignores the structure provided by the claim itself. Claim 1 of the ’517 patent requires:

- “storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence”
- “storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules”
- “identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application”
- “identifying, by a runtime monitor including a processing device, a behavior score for the application program that executes on the device based on the identified runtime risk”
- “wherein the action sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action”

PAN again oversimplifies the claim and overlooks elements in arguing the claim is “analogous to a human assigning a credit score or rating based on a predefined algorithm.” Motion

at 9. PAN ignores that the “performed actions” of the “action sequence” identified in each of the “plurality of rules” are one of at least “a user action, an application action, and a system action.” Aside from a “user action,” these claimed actions are clearly not human activities, and are necessarily linked to the computer system. Claim 1 further requires that “a runtime monitor including a processing device” identify “a behavior score for the application program that executes on the device based on the identified runtime risk.” The runtime monitor is integral to the claim, as it includes a processing device that implements the identification of the behavior score. PAN fails to address this, and merely states that assigning a “‘behavior score,’ based on known (but unspecified) ‘rules’ and ‘policies,’ [] could be assessed mentally by a human.” Motion at 10.

PAN also identifies steps performed by the claimed application program without explaining how a human could possibly perform them. In particular, PAN notes the method requires that “rules” corresponding to an “action sequence” be stored, and that “assessment policies” be stored. *Id.* at 10. PAN fails to explain the meaning of these terms in its analysis, highlighting the need for claim construction to decide patent eligibility.

PAN’s attempt to analogize *Dropbox, Inc. v. Synchronoss Techs., Inc.* 815 F. App’x 529,532 (Fed. Cir. 2020) is misplaced. Motion at 10. The representative claim in *Dropbox* claimed only the retrieval of “a sensitivity level” and “a trust level,” and an “access checker” that could provide access to a resource if “the trust level . . . is sufficient for the sensitivity level.” *Id.* Thus, the claims merely compared two received values, which a human could do. In contrast, Claim 1 of the ’517 patent requires a runtime monitor that identifies a behavior score which is based on a runtime risk of an application program. The runtime risk is not simply a static value that is received (as in *Dropbox*), but it is determined based on user actions, application actions, and system actions.

The numerous types of system and application actions are discussed below, showing that the claimed method of assessing runtime risk could not be performed by a human.

Immediately after arguing that Claim 1 only contains steps that could be performed by a human, PAN reverses course and alleges that it can't determine "**how**" the steps of Claim 1 are performed. Motion at 11. The claims are read in light of the specification, and PAN's argument merely demonstrates that claim construction is needed to understand the scope of the claims. *Bancorp Servs., L.L.C. v. Sun Life Assur. Co. of Can.*, 687 F.3d 1266, 1273-74 (Fed. Cir. 2012).

Claim 1 of the '517 patent is also not directed to routine, well-known, and conventional ideas under *Alice* Step Two, and factual issues remain regarding the state of the art at the time the patent was filed. *Ollnova*, Slip Op. at 17-18. PAN cites no prior art or expert testimony supporting its position. While "antivirus programs, firewalls, and intrusion detection/prevention systems" were known in the prior art, "[e]merging cyber threats, commonly referred to as advanced persistent threats (APT), often remain undetected" by these programs and systems. '517 patent, 1:19-28. In view of the shortcomings of these traditional security programs, the '517 patent presented "a technical solution to properly detect and prevent attacks by advanced persistent threats." *Id.*, 1:36-37. PAN seeks to reduce the inventive concept of the '517 patent to a handful of singular claim terms, arguing that "The 'rules,' 'policies,' 'runtime risk,' 'behavior score,' and 'actions' are all in the abstract realm," but without even addressing the meaning of these terms (many of which require construction). Motion at 12. PAN's efforts to reduce the claim limitations to single words ignores the innovative usage of the runtime monitor described in the '517 patent which identifies a behavior score based on an identified "runtime risk." Also, the "rules" noted, but explained, by PAN are based on identified "action sequences" that include actions of "an

application” and “a system.” The specification explains the application and system actions as follows,

The application action 304 may include, for example, a start type (e.g., console, service, parent process, script), first time execution, fork process (e.g., child process creation), code injection methods, keyboard capture methods, screen capture methods, dynamic code blocks, open data documents, automatic or self-termination, abnormal terminations (e.g., exception conditions), multiple restarts, opening of device(s) (e.g., the device for which the runtime risk is identified), process enumeration, cryptography, communication protocols, performance metrics, etc. as will be apparent to persons having skill in the relevant art.

’517 patent, 7:4-14.

The system action 306 may include, for example, system file creation, system folder modification, registry modifications or additions, application setting modifications, driver install or uninstall (e.g., system files), network activity, execution from temporary system folders, alternate data streams (ADS), environmental aspects (e.g., debugger presence, virtual environments, system boot times/sequences), etc.

*Id.*, 7:19-26.

The steps of the ’517 patent can only be performed with the claimed processing device and show that the claims of the ’517 patent were not well-known, routine, or conventional at the time of the invention.

#### **D. The ’038 and ’918 Patents are Patent-Eligible Under 35 U.S.C. § 101**

Plaintiff mischaracterizes the claims of the ’038 patent (attached as Exhibit 4) and ’918 patent (attached as Exhibit 5) as merely “determining compliance with a policy and restricting access, which is akin to limiting access to a bridge or highway based on paying a toll or carpool/HOV requirements.” Motion at 1. This over-genericizes and ignores the inventive concepts of the claim. For example, Claim 1 of the ’038 patent and claim 1 of the ’918 patent require:

- “providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies”

- “maintaining the plurality of policies in a data store on the computing system”
- “identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to evaluate”
- “configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions”
- “receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint” (’918 patent)
- “receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents” (’038 patent)
- “determining, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store”
- “authorizing access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state” (’918 patent)
- “initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint” (’038 patent)
- “continuing to monitor the compliance state by the endpoint and restricting access to the computing resource if the compliance state changes” (’918 patent)

PAN improperly reduces these claims to merely “determining or conditioning access on compliance with a policy” in a blatant attempt to manufacture factual similarities with dissimilar caselaw. Motion at 12. But these patents are directed to far more than mere access based on compliance with a policy. The ’038 patent and the ’918 patent realized that even the latest prior art access control solutions “still lack[ed] significant functions and capabilities,” such as “the ability to form context-based access control decisions using as decision inputs state information provided by point solutions that are not context aware” and “the ability to collect endpoint state information from multiple point solutions, collect endpoint state information from the environment itself (*e.g.* information obtained from the operating system), and integrate the collected information to form a higher-level holistic and intelligent view of the overall endpoint state,” among many others. ’038 patent, 3:1-10; ’918 patent, 3:7-17. The patents addressed these shortcomings by

providing for “flexibly managing corporate security policies, typically to control access to local or remote computing resources.” *Id.*, 3:36-38; ’918 patent. 3:43-45. To provide this capability, the claims require a remote user interface for “configuration of a plurality of policies” that are maintained in a data store, identifying “a plurality of operating conditions on the endpoint to evaluate,” and “configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions.” The “software services” and “software agents” on the endpoints gather “status information about the plurality of operating conditions.” The computing system then determines “a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store.” ’038 patent, claim 1; ’918 patent, claim 1. Only after these steps are implemented by the computing system can an action be initiated (’038 patent) and access be authorized (’918 patent). Under *Alice* Step One, the claims are not directed to an abstract idea.

This case is analogous to both *Enfish, LLC*, 822 F.3d at 1336 and *eCeipt LLC v. Homegoods, Inc.*, No. W-19-CV-00032-ADA, 2019 WL 10302271, at \*5 (W.D. Tex. May 20, 2019), as “the plain focus of the claim[ ] is on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity.” Like the claims in those cases, the claims here are not directed to abstract ideas because they “provide[] a series of specific steps that creates a practical improvement to the operation and functionality of prior [computer] systems.” *Id.*

The claims are also not well-known, routine, and conventional under *Alice* Step Two. PAN again attempts to parse out the claims into simple “recited categories of information,” and then allege that the “computer and network components are all conventional.” Motion at 15. The Federal Circuit has repeatedly cautioned against mischaracterizing and disregarding claim

elements, as PAN has done here. *TecSec, Inc.*, 978 F.3d at 1295 (citing *Enfish, LLC*, 822 F.3d at 1337). PAN provides no explanation or analysis showing that the claims’ *combinations* of elements were well-known, routine, and conventional, and cites to no prior art or expert testimony to support this proposition.

The ’038 patent and ’918 patent “provide[] new and improved methods and systems for flexibly monitoring, evaluating, and initiating actions to enforce security compliance policies.” ’038 patent, 6:36-39; ’918 patent, 6:44-46. The patents provide a “policy management system 106 is seen to include a compliance analysis engine 106C as well as various policy information stored within storage system 106B.” ’038 patent, 8:14-16; ’918 patent, 8:23-26. The “compliance analysis engine 106C, typically comprising software in data store 106B running on hardware 106A, functions to receive system condition information and process that condition information in accordance with the security policies, such as are stored within data storage 106B, in order to generate security rules.” *Id.*, 8:17-22. ’918 patent, 8:26-32. In addition to the capability of generating security rules, the claims require that an action identified in the rule is “carried out by the processor on the endpoint.” The claims here are again comparable to those in *Finjan*, where the court found a method for scanning an application program for viruses, generating a security profile identifying any potentially suspicious code in the program, and linking the security profile to the application program constituted an improvement in computer functionality, and therefore held included an inventive step making the claims patent eligible. *Id.* at 1304–05.

#### **IV. CONCLUSION**

Because each challenged patent claims eligible subject matter, Defendants respectfully request that Palo Alto Networks, Inc.’s Motion for Partial Judgment on the Pleadings of Patent-Ineligibility Under 35 U.S.C. 101 (Dkt. 71) be denied in its entirety.

Dated: January 18, 2023

Respectfully submitted,

/s/ Alfred R. Fabricant

Alfred R. Fabricant

NY Bar No. 2219392

Email: ffabricant@fabricantllp.com

Peter Lambrianakos

NY Bar No. 2894392

Email: plambrianakos@fabricantllp.com

Vincent J. Rubino, III

NY Bar No. 4557435

Email: vrubino@fabricantllp.com

Joseph M. Mercadante

NY Bar No. 4784930

Email: jmercadante@fabricantllp.com

**FABRICANT LLP**

411 Theodore Fremd Avenue,

Suite 206 South

Rye, New York 10580

Telephone: (212) 257-5797

Facsimile: (212) 257-5796

Justin Kurt Truelove

Texas Bar No. 24013653

Email: kurt@truelovelawfirm.com

**TRUELOVE LAW FIRM, PLLC**

100 West Houston Street

Marshall, Texas 75670

Telephone: (903) 938-8321

Facsimile: (903) 215-8510

Jennifer L. Truelove

Texas State Bar No. 24012906

Email: jtruelove@mckoolsmith.com

**MCKOOL SMITH, P.C.**

104 E. Houston Street, Suite 300

Marshall, Texas 75670

Telephone: (903) 923-9000

Facsimile: (903) 923-9099

**ATTORNEYS FOR DEFENDANTS**

**TAASERA LICENSING LLC and**

**QUEST PATENT RESEARCH CORPORATION**

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that, on January 18, 2023, all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3).

/s/ Alfred R. Fabricant

Alfred R. Fabricant